Risk Based Approach to Vulnerability Management Program

Kumar Ravi
Vice President - Information Security & Data Privacy
EXL Service

What Would Be A Good Vulnerability Management Program

It is always *GOOD* to know your weaknesses…..

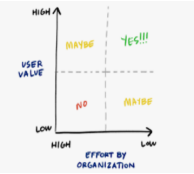
…… and its the *BEST* to timely take care of them!

Minimize the Risk around Vulnerable Systems and Vulnerabilities by helping you ***rightly and quickly identify*** the vulnerabilities and helping you ***prioritize efforts*** towards the ***high risk items first.***

Areas of Focus for a Good Vulnerability Management Program

Sound Inventory Management System & Practices (A)

Speed and Efficacy of Vulnerability Identification (B)



Risk Prioritization around Relevant Aspects (C)

Promptness in Remediation (D)

Important Questions To Get You There

A

Is my inventory up-to-date always?

B

How soon I get to know about my vulnerable systems?

C

Which are the potential low hanging fruits?

D

How much time I have to patch the vulnerabilities?
- SLA for Closure

Which are my important assets?
- Crown Jewels

Which all systems are suffering from critical vulnerabilities?

Which are being exploited globally?

Is there enough bandwidth to patch all vulnerabilities?

Which of my important assets are significantly vulnerable?

Are these vulnerabilities confirmed?

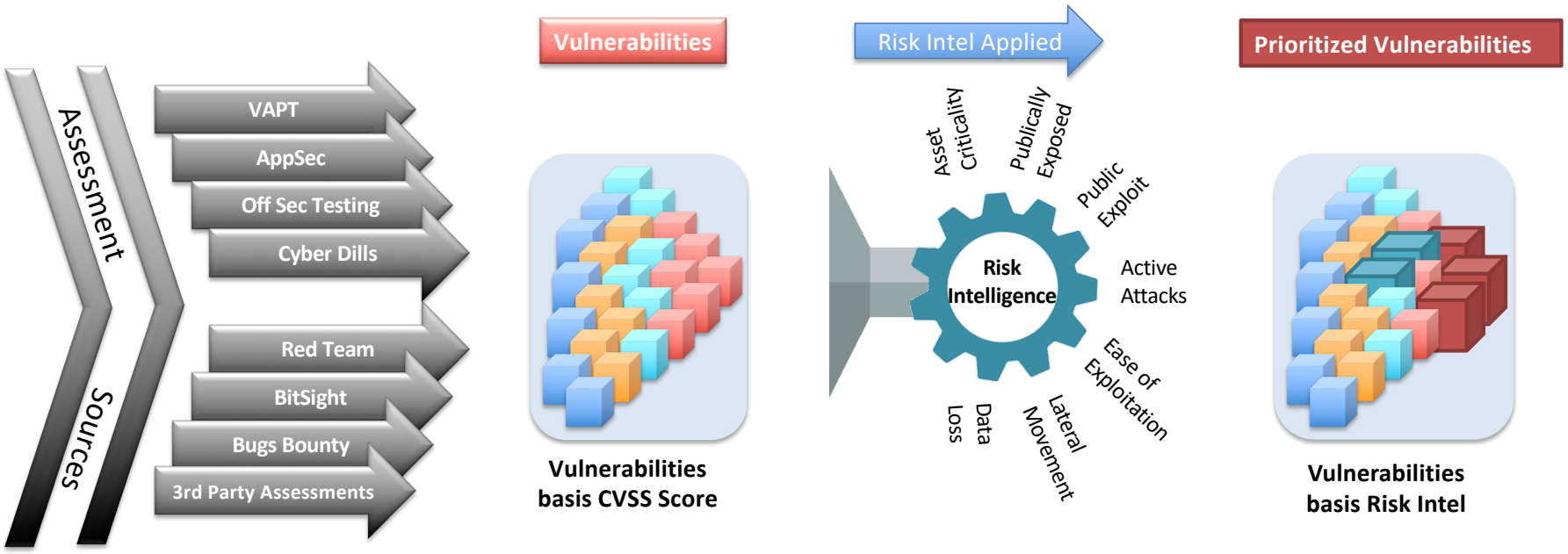
Which vulnerabilities have known exploit available for?

So, which vulnerabilities should I patch first?

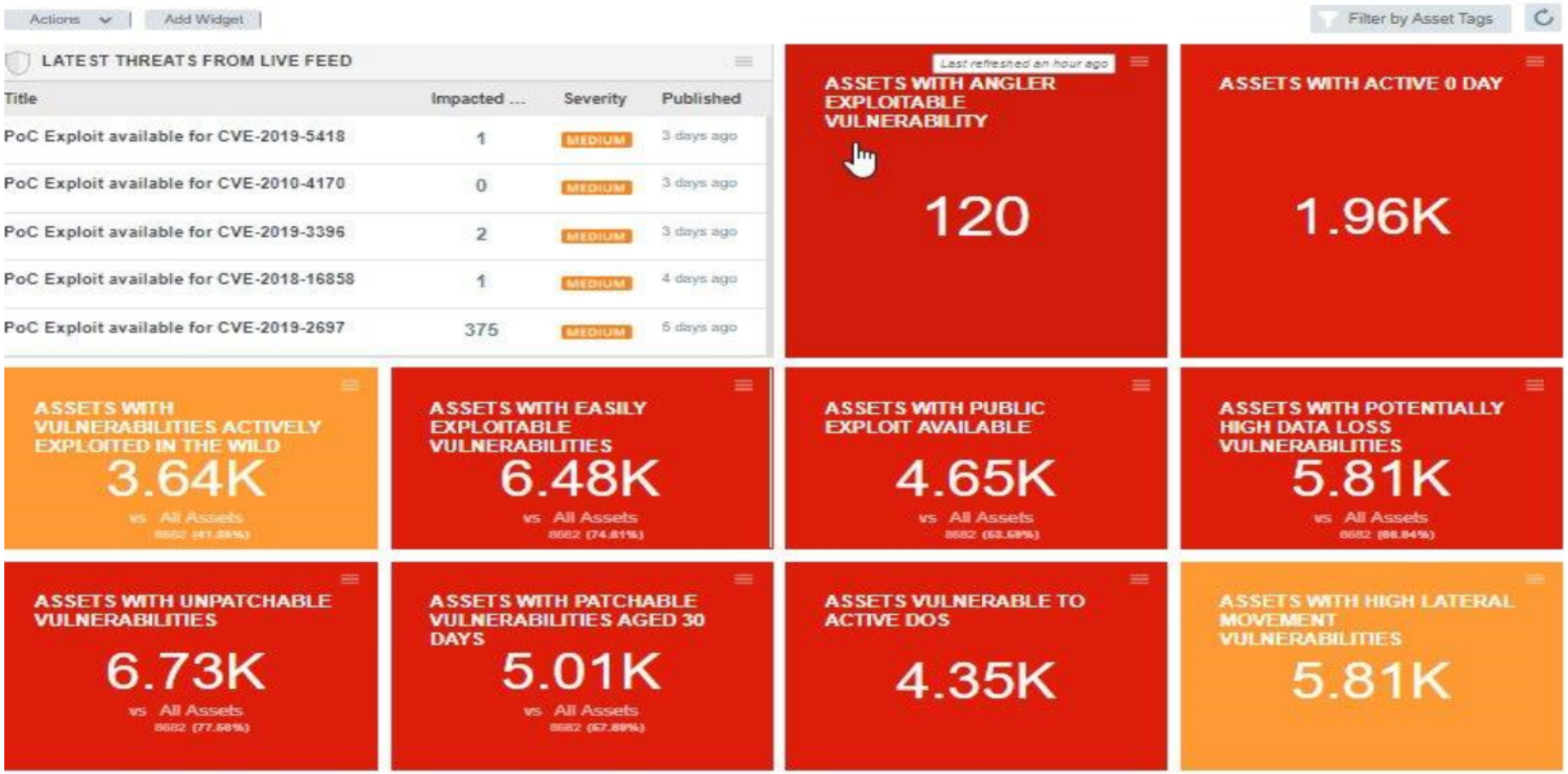
EXL's Vulnerability Management Program Maturity Synopsis

Maturity Dimensions	Erstwhile Practices	Maturity Steps
Coverage *Which all systems are under scope*	All Production Environment	Both - Prod and Non-Prod
Depth *Outside vs inside view*	Unauthenticated Scans Remote scanning	Authenticated Scans Local (Cloud Agent) scanning Policy Compliance
Frequency *How soon to assess the environment*	Periodic (YY→QQ→MM)	Real-time
Independence *Who should do the assessments*	InfoSec Team	Technology Team→ InfoSec Team
LifeCycle *Pre-Production vs Post-Production*	Ongoing	Pre-Production + Ongoing
Response Priority *Which one to focus on*	Same SLA for Internal & External + Critical and High Severity + Public Facing	Differentiated SLAs + Asset Criticality (Context) + **Risk Intelligence** (Context) + **Threat Intel** (Context)

Risk and Context Driven – Remediation Approach



RISK VIEW OF THE VULNERABILITIES



Next Level - Risk Intel + Threat Intel

Fire Eye GTI

HP RepSM

Malware Analysis

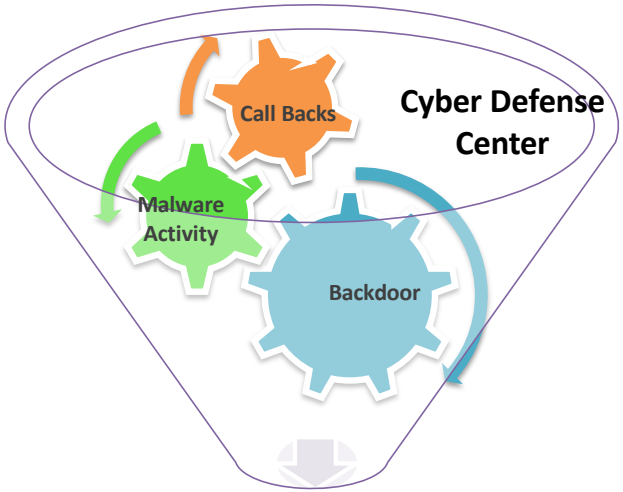
MSSP Intel

Vulnerabilities basis

Risk Intel

Risk Intel

Threat Intel



Risk Intel + Threat Intel = P0 Tickets

ACHIEVED BENEFITS

- **Comprehensive** Coverage of Threat Landscape
- **Real Time** Risk Status & Dashboard
- Lesser **False Positives**
- Prioritized **Real Critical Risks** Remediation
- Self Capable Technology Team – **no dependency** on InfoSec team
- **Quick** Identification, Remediation and Validations
- Centralized ***Policy Compliance*** management
- **Higher Team Efficiency** through Technology Automation and Process Enhancement

THANK YOU